Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (previously presented) A method of ensuring the security of a patient's results from a medical test conducted by a laboratory, the method comprising:

    providing the patient with a medical data card containing a unique patient identification number;

    taking a specimen from the patient for conducting the medical test;

    generating a first medical test request containing the unique patient identification number using the patient's medical data card; and

    transmitting the specimen and the first medical test request to a secure data provider, wherein the secure data provider generates a second medical test request devoid of publicly accessible patient identification information using the first medical test request, transmits the specimen and the second medical test request to the laboratory, receives the results from the medical test from the laboratory, and reports the results on a test results card that can only be read in conjunction with the patient's medical data card.

2. (previously presented) The method according to claim 1 further comprising reading the results on the test results card using the patient's medical data card.

3. (previously presented) The method according to claim 1 wherein the patient's medical data card includes a memory, and further comprising the step of storing the results in the memory on the patient's medical data card.

4. (original) The method according to claim 1 wherein the patient identification number is not readable from the patient's medical data card without a PIN, and wherein the step of generating the first medical test request includes the patient supplying the PIN.

5. (previously presented) The method according to claim 2 wherein the results are not readable with the medical data card without a PIN, and wherein the step of reading the results on the test results card includes the patient supplying the PIN.

6. (previously presented) A method of ensuring the security of a patient's results from a medical test conducted for a medical provider by a laboratory, the method comprising:

    issuing the patient a medical data card containing a unique patient identification number;

5   receiving from the medical provider a first medical test request generated using the patient's medical data card and a patient specimen for use in conducting the medical test;

    generating a second medical test request using the first medical test request, the second medical test request being devoid of publicly accessible information about the identity of the patient;

10   forwarding the second medical test request and the specimen to the laboratory for conducting the medical test;

    receiving the results of the medical test from the laboratory; and

    providing the results to the medical provider in a form that can only be read in conjunction with the patient's medical data card.

15

7. (previously presented) The method of claim 6, wherein the results are on a test results card in computer readable form and the method further comprises providing the medical provider with a reader adapted for reading the tests results.

20   8. (previously presented) A medical data card for use in a system for ensuring the security of a patient's results from a medical test conducted for a medical provider by a laboratory, the medical data card including:

    a unique patient ID code,

    a public key encryption private key,

25   a public key encryption public key, and

    a data storage element, wherein the data storage element is adapted for storing data for at least one medical test, including for each medical test: a medical test type, a unique identification code for the medical test on the patient, and the results of the medical test.

30   9. – 17. (canceled)

18. (previously presented) A method of ensuring the security of a patient's results from a medical

test conducted for a medical provider by a laboratory, the method comprising:

issuing the patient a medical data card containing a unique patient identification number;

receiving from a medical provider a first medical test request generated using the patient's medical data card and a patient specimen for use in conducting the medical test;

5   generating a second medical test request using the first medical test request, the second medical test request having encrypted information identifying the patient but being devoid of publicly accessible information about the identity of the patient, and including a public encryption public code specific to the patient;

forwarding the medical test second request and the specimen to the laboratory for 10   conducting the medical test;

receiving the results of the medical test from the laboratory, wherein the results are encrypted using the public encryption public code on the second medical test request;

identifying the patient to whom the results pertain; and

providing the encrypted results to the medical provider, wherein the encrypted results can 15   only be decrypted in conjunction with the patient's medical data card.

19. (previously presented) A method of ensuring the security of a patient's results from a medical test conducted for a medical provider by a laboratory, comprising:

providing the patient with a medical data card issued by a secure information provider, 20   having a unique patient identification number, a public key encryption private key, and a public key encryption public key;

taking a specimen from the patient for conducting the medical test;

generating a first medical test request using the patient's medical data card, the first medical test request including an encrypted identification of the patient and the medical test; 25   a code identifying the medical provider; the patient identification number; the public encryption public key; and an identification of a medical test type;

forwarding the first medical test request and the specimen to the secure information provider;

generating a second medical test request including an encryption of the patient's unique 30   patient identification number, but otherwise devoid of any indicia that would identify the patient, and an encryption code;

forwarding the second medical test request and the specimen to the laboratory, wherein

the laboratory conducts the medical test and provides the results of the medical test in
encrypted form using the encryption code on the second medical test request;

receiving the encrypted results;

identifying the medical provider from encrypted information included with the encrypted

5   results;

forwarding the encrypted results to the medical provider with an identification of the
patient; and

decrypting the encrypted results using the patient's medical data card.